

Entorno personal de aprendizaje:

Curso de Gestión de Servicios en la Nube



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

 **GOBIERNO
NACIONAL**

*Paraguay
de la gente*

Unidad 6.**Servicios básicos en la nube: Gestión de Contraseñas en línea**

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Viceministerio de Tecnologías de la Información y Comunicación

Dirección General de Inclusión Digital y TIC en la Educación

Información

SEDE 1



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

Dirección: Complejo Santos E2 - Gral. Santos 1170 c/ Concordia

Teléfono: (+595 21) 217 9000

Correo electrónico: comunicacion@mitic.gov.pyMesa de entrada: sgeneral@mitic.gov.py

Asunción – Paraguay

Servicios básicos en la nube: Gestión de Contraseñas en línea

Todas las imágenes presentes en este material de apoyo educativo han sido reconocidas y, en todos los casos, son de uso libre, o bien son Creaciones e imágenes propias de los autores del material, cuando no haya referencia en contrario.

Obra publicada con licencia de Creative Commons Reconocimiento-Compartir Igual 4.0

<https://creativecommons.org/licenses/by-sa/4.0/>



Unidad 6.**Servicios básicos en la nube: Gestión de Contraseñas en línea****Tabla de contenido**

1.	Fundamentos de la gestión de contraseñas en línea.....	4
2.	Gestores de contraseña integrados en navegadores web.....	6
3.	Gestores de contraseña en línea como servicio	9
4.	Referencias	22

Unidad 6.

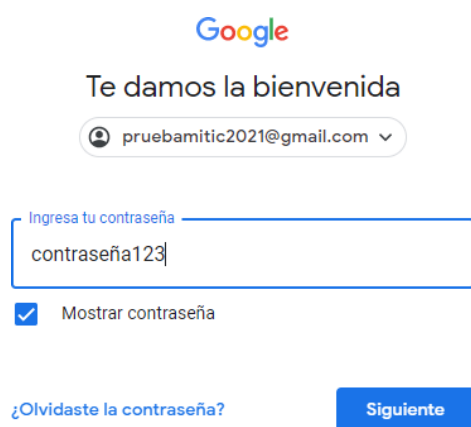
Servicios básicos en la nube: Gestión de Contraseñas en línea

Servicios básicos en la nube: Gestión de Contraseñas en línea

1. Fundamentos de la gestión de contraseñas en línea

En el mundo tecnológico de hoy, no es posible como usuarios permitirnos el lujo de que nuestras **contraseñas** (los famosos “*password*”, por su denominación en inglés), aquellas que dominan nuestra huella digital, nuestros correos personales y laborales, nuestra agenda profesional, nuestros recuerdos, nuestra cuenta bancaria, (y los ejemplos son interminables) tengan vulnerabilidades simples, y que sean fácilmente descubiertas por personas maliciosas, pues de esta manera podemos tener consecuencias catastróficas, como la pérdida de nuestros ahorros, la suplantación digital de identidad, el secuestro de nuestros datos importantes (con un pedido especial de rescate, generalmente económico, conocido como “ransomware”) y otros similares.

En el caso de usuarios descuidados, utilizan para estos fines combinaciones sencillas de descubrir como “12345”, “contraseña”, “password”, los números de la propia fecha de nacimiento (por ejemplo “30111985”) o bien el nombre de la pareja, de alguno de los hijos o los padres, alguna combinación de estas informaciones, etc. de tal forma que un atacante puede descubrirlo con un intento muy limitado de posibilidades obvias con un poco de información en línea disponible; todo ello sin obviar que generalmente las formas de recuperación de contraseñas de muchos sitios en línea populares, solicitan información en teoría privada a los usuarios para proceder a generarles nuevas contraseñas, pero obviando que muchos ponen ese tipo de información al alcance de virtualmente cualquiera, a través de las redes sociales.



Google

Te damos la bienvenida

 pruebamitic2021@gmail.com ▼

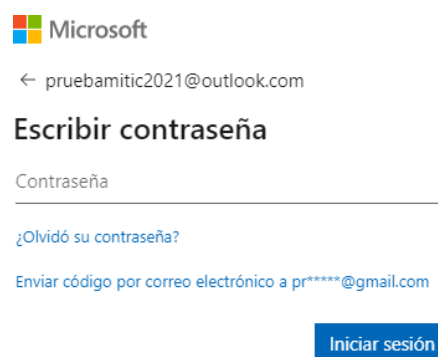
Ingresa tu contraseña

contraseña123

☒ Mostrar contraseña

[¿Olvidaste la contraseña?](#)

[Siguiente](#)



Microsoft

← pruebamitic2021@outlook.com

Escribir contraseña

Contraseña

[¿Olvidó su contraseña?](#)

[Enviar código por correo electrónico a pr*****@gmail.com](#)

[Iniciar sesión](#)

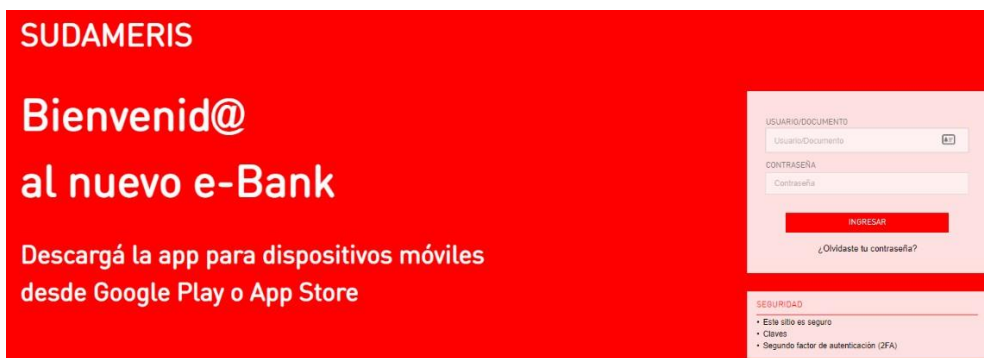
Unidad 6.

Servicios básicos en la nube: Gestión de Contraseñas en línea

Si estamos leyendo el material de un curso como este, es muy posible que nos consideremos usuarios un tanto más avanzados que aquellos, pero posiblemente choquemos con otro muro: no es recomendable jamás utilizar la misma contraseña para distintos servicios. Esto es así, porque en caso de que uno de los servicios en los cuales la utilicemos sea vulnerado, entonces nuestros datos pueden ser expuestos (por ejemplo si el servicio online de correo que utilicemos llega a ser “hackeado” o lo que es lo mismo, vulnerado, entonces TODOS los servicios en los cuales utilicemos la misma contraseña están en peligro, pues los atacantes pueden vincular a través de nuestros datos a tales servicios, e ir probando con cuáles funcionan las contraseñas robadas) y eso implica que deberíamos utilizar una contraseña diferente para cada servicio; si hacemos una lista rápida tenemos que normalmente una persona tiene al menos los siguientes servicios en línea hoy en día:

- Cuenta de correo electrónico (Gmail, Hotmail, Outlook, iCloud, y otros)
- Cuenta Bancaria (Sudameris, GNB, BNF, Itaú, Continental, y otros)
- Perfiles en Redes Sociales (Twitter, Facebook, Instagram, TikTok, y otros)
- Usuario de servicios de noticias (ABC, Última Hora, La Nación, y otros)
- Usuario de páginas de compras de servicios y mercaderías online (Amazon, Ali Express, Mercado Libre, Clasipar, y otros)
- Usuario de gestión académica en la universidad, colegio u otra entidad educativa
- Usuario de ingreso a la red laboral, con gestión de información delicada
- Perfil en servicios de tiendas de aplicaciones, con información y uso de tarjetas de crédito vinculadas (Play Store, Apple Store)

Todo ello sin contar que, además, muchos de estos servicios nos piden renovar la contraseña cada cierto periodo de tiempo, y además, para que una contraseña pueda ser considerada “segura” generalmente debe mezclar números, letras tanto mayúsculas y minúsculas, así como símbolos y todos ellos en orden aleatorio.



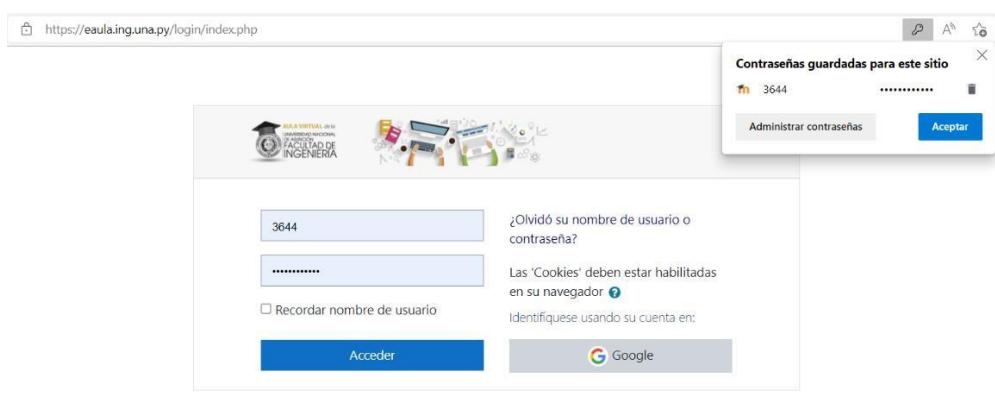
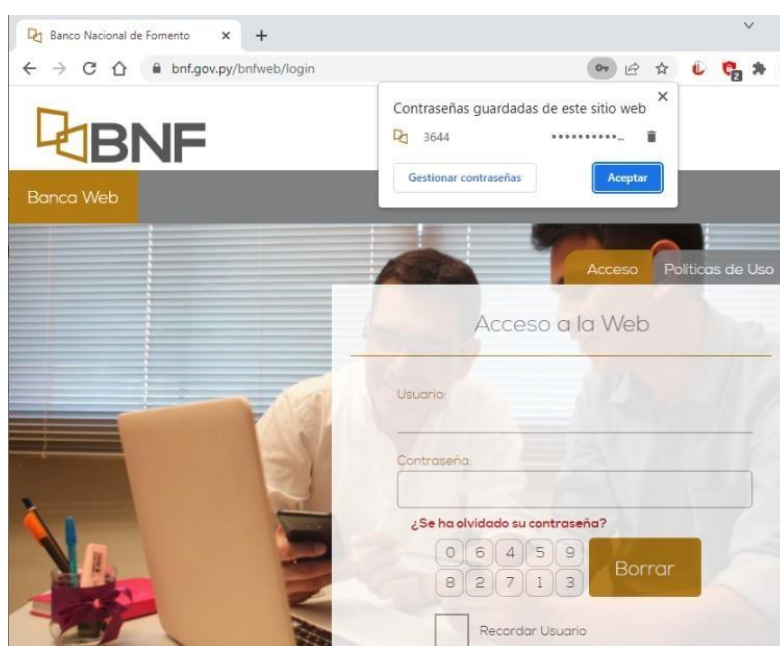
Unidad 6.

Servicios básicos en la nube: Gestión de Contraseñas en línea

Por todo esto, en un momento dado se torna más que necesario poseer alguna herramienta que nos ayude a gestionar las contraseñas tanto en todos los navegadores, computadoras tanto laborales y personales, así como dispositivos móviles como teléfonos y hasta relojes inteligentes que vayamos a utilizar.

2. Gestores de contraseña integrados en navegadores web

Considerando lo planteado anteriormente, se puede tener en cuenta que los navegadores web tradicionales (Google Chrome, Microsoft Edge, y otros) poseen sus propios gestores de contraseña, pero ellos más bien se encargan de “recordar” en ciertos sitios, las credenciales de usuario y contraseña que vayamos cargando, pero no de generar contraseñas, o realizar sugerencias (o al menos, esta no es su característica fuerte), y están atados a que utilicemos el mismo navegador en todos los dispositivos. Estos gestores generalmente integran algún botón con símbolo de llaves en el navegador, y recuerdan la información si nosotros se lo permitimos.

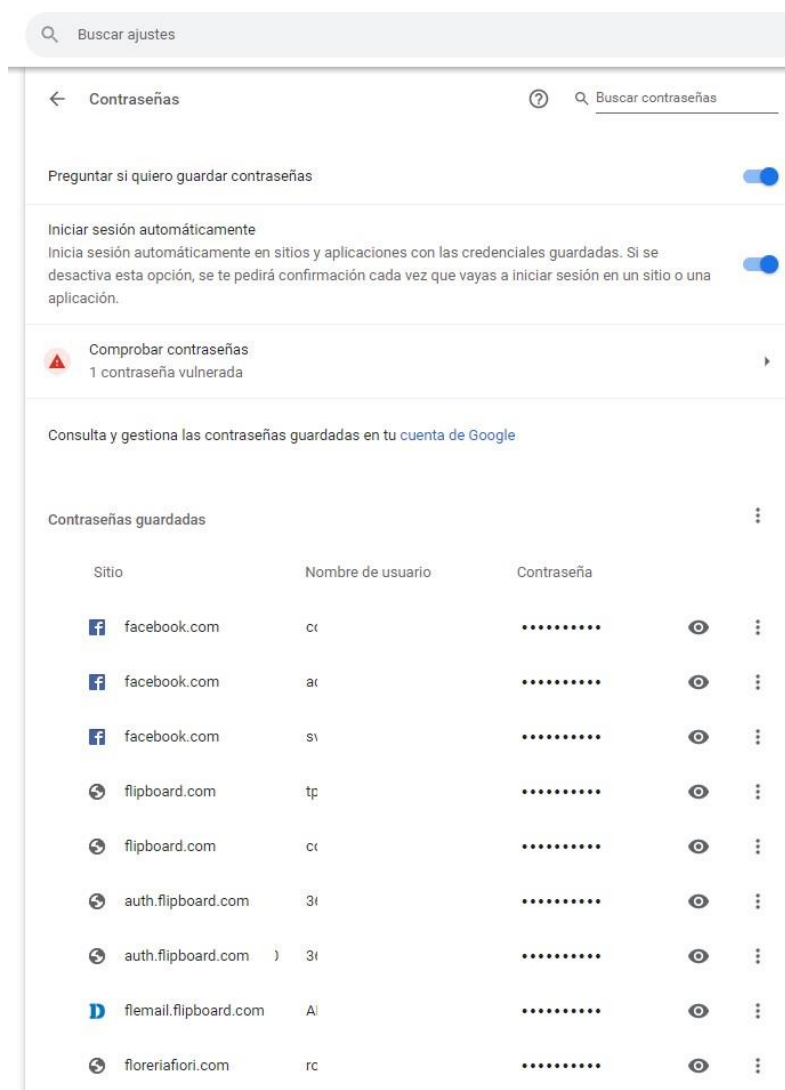


Unidad 6.

Servicios básicos en la nube: Gestión de Contraseñas en línea

En concreto, al ingresar a un sitio web dado desde un dispositivo (o varios, puede ser desde la computadora de escritorio o el móvil, por ejemplo), con nuestro usuario y contraseña, el navegador nos ofrece “recordar” los mismos, a lo cual si nos es conveniente usualmente lo podremos aceptar. El problema radica en que una vez que alguien tiene acceso a dichos dispositivos (por ejemplo, a nuestra computadora laboral, con la misma sesión abierta de nuestro usuario particular) puede tener disposición de cualquiera de esos datos confidenciales.

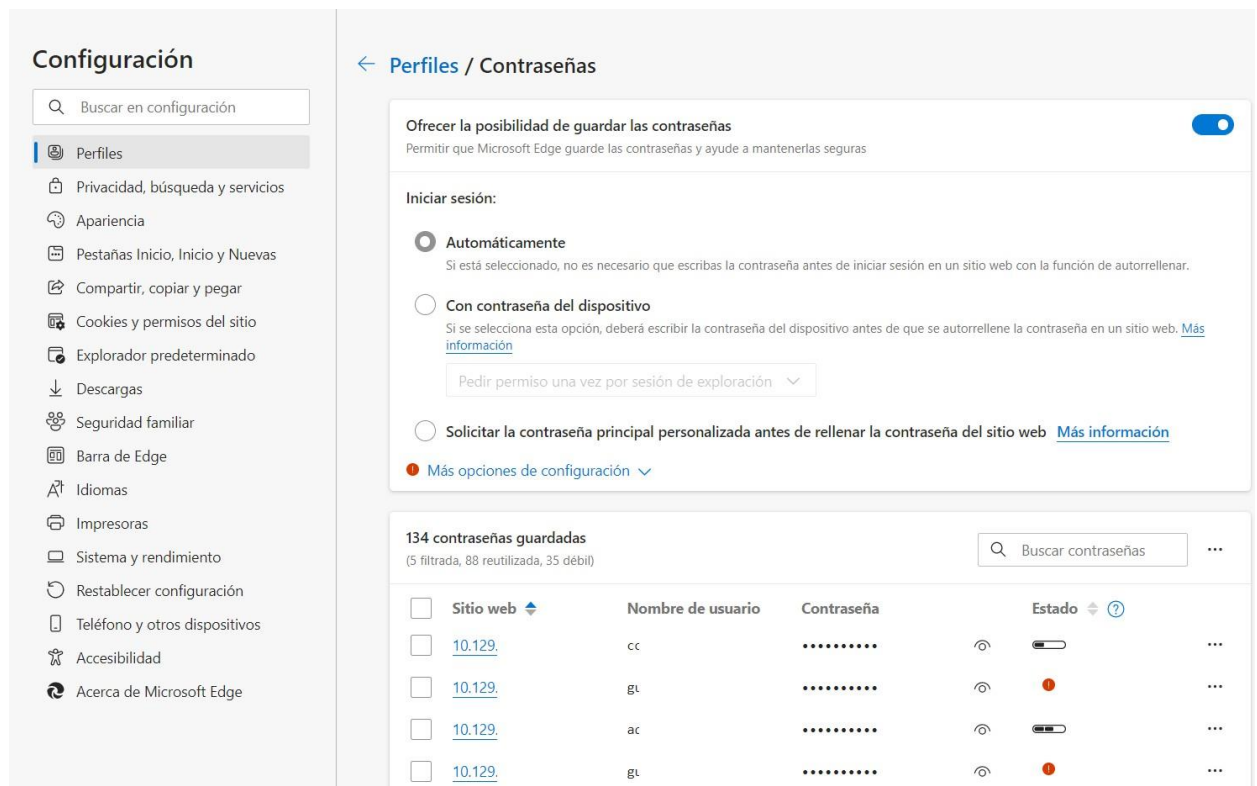
Por caso, en Google Chrome si damos clic al botón de “llave” y luego a “Gestionar contraseñas”, nos encontraremos con una lista de contraseñas a las cuales hayamos dado la indicación de recordarlas en el gestor del navegador:



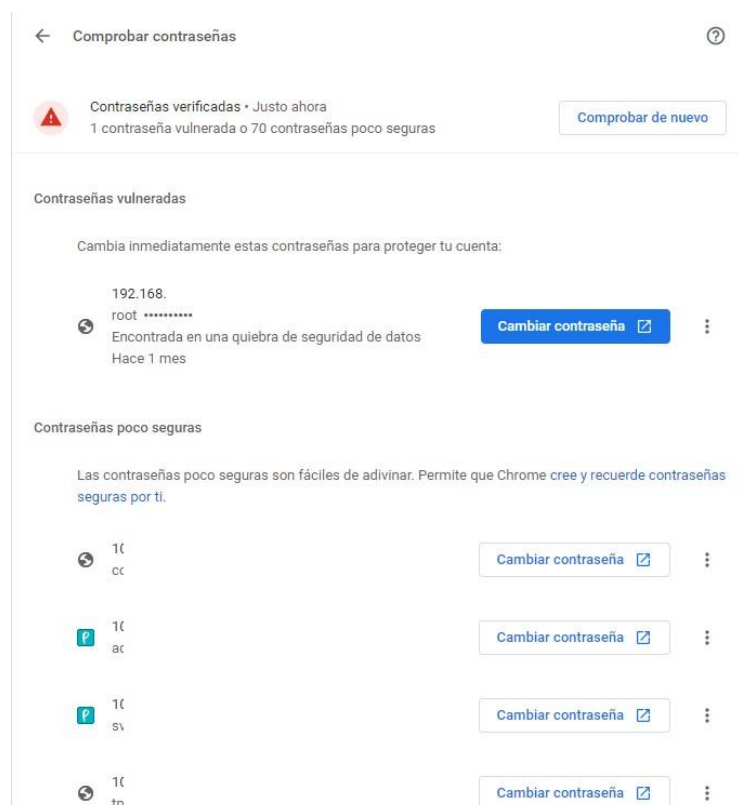
En el caso de Microsoft Edge, ofrece las mismas posibilidades haciendo uso de la opción “Administrar contraseñas” al darle clic al botón de llave de la barra de navegación, desplegando la lista de sitios cuya contraseña se tiene guardadas y asociadas al perfil del usuario en cuestión.

Unidad 6.

Servicios básicos en la nube: Gestión de Contraseñas en línea

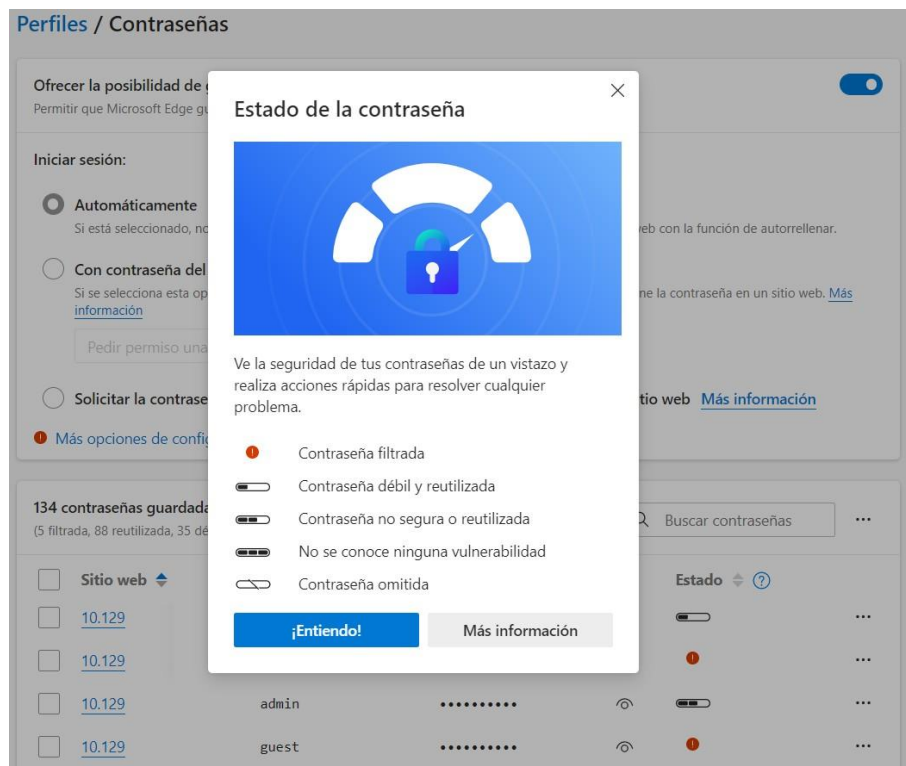


En ambos casos de ejemplo, los gestores permiten también verificar el nivel de seguridad de las contraseñas, en cuanto a parámetros de seguridad, o bien si las mismas incluso fuesen filtradas en algún ataque público y deban ser cambiadas.



Unidad 6.

Servicios básicos en la nube: Gestión de Contraseñas en línea



En suma, los gestores de contraseñas integrados en los navegadores tienen una serie de posibilidades interesantes, pero que resultan muy limitadas en comparación con las que ofrecen los gestores de contraseña puramente en línea, que veremos a continuación.

3. Gestores de contraseña en línea como servicio

Una ampliación de las posibilidades, la logran los gestores de contraseña como servicio dedicado, que ofrecen tales características a través de sitios web (desde el navegador) pero integrando también la posibilidad de utilizarlos en los dispositivos móviles, a través de la aplicación correspondiente.

En general, este tipo de servicios suelen tener modalidades gratuitas o bien de pago (con más posibilidades y suelen añadir características más detalladas) pero las que analizaremos aquí son las versiones gratuitas, de adopción más generalizada.

Estos servicios permiten guardar contraseñas para utilizarlas en cuanto sea necesario, y además (lo más resaltante) ayudan a generar contraseñas de forma aleatoria y que cumplan con los estándares de seguridad requeridos, para almacenarlas posteriormente. Además pueden incluir

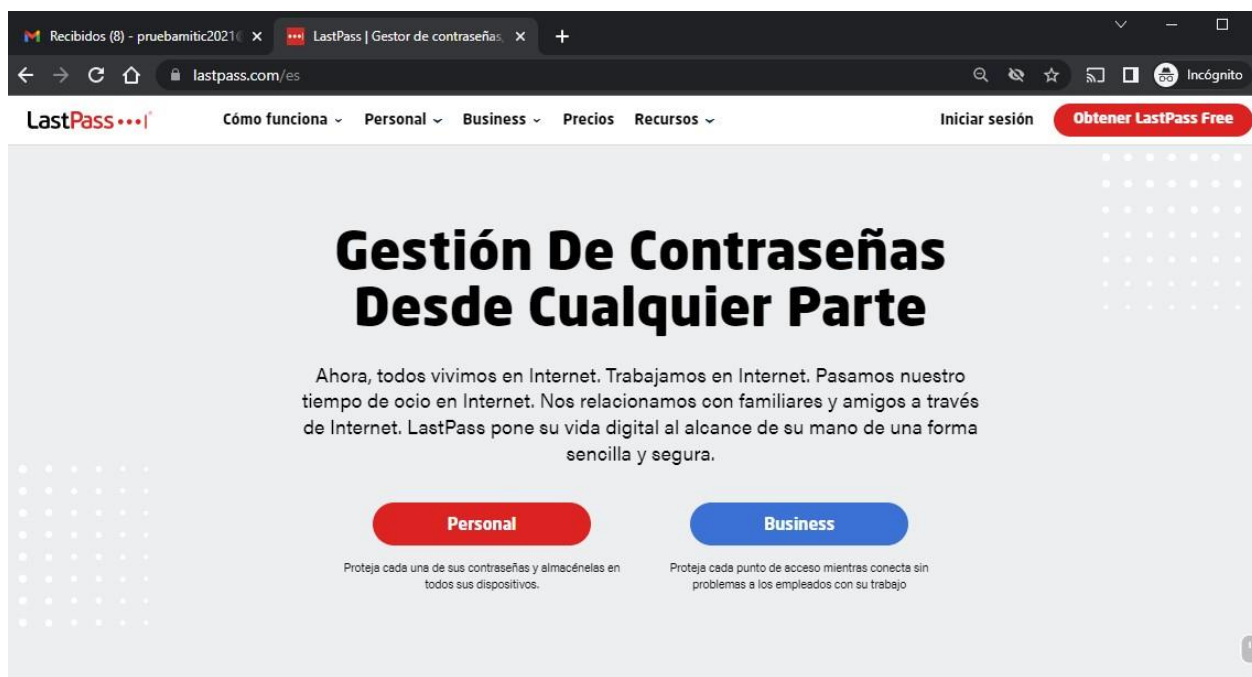
Unidad 6.

Servicios básicos en la nube: Gestión de Contraseñas en línea

alertas de aviso para cuando las contraseñas que el propio usuario genere sean débiles en cuanto a patrones y diversidad de caracteres, o bien, estén siendo repetidamente utilizadas en varios sitios. En general, su fortaleza radica en también sincronizarse en la nube, caso parecido a los gestores integrados de los navegadores que ya analizamos, pero con la ventaja de que no se necesita tener instalado el mismo navegador en todos los dispositivos, ya sea la computadora de escritorio, teléfono móvil y cualquier dispositivo en el que se desee utilizarlos.

Vamos a mencionar como referencia a 2 servicios bastante conocidos, de modalidad gratuita, y sus características y modo de uso.

El primer servicio, y tal vez el más famoso a nivel gratuito es **“LastPass”**. Aunque también tiene versión de pago con funciones más avanzadas, en su versión gratuita nos permite tener todas las funciones esenciales de generación y almacenamiento de contraseñas; funciona directamente desde el navegador web que estemos utilizando, sea cual sea este. Para utilizarlo, se debe ingresar al sitio web: <https://www.lastpass.com/es>, y crear una cuenta asociada al servicio haciendo un clic en el botón “Obtener LastPass Free”.



Piloto automático para todas sus contraseñas

LastPass le permitirá olvidarse de complicados procedimientos para recuperar contraseñas y dedicar ese tiempo a disfrutar de las cosas que más le gustan.

Una vez realizado esto, ingresamos el correo con el cual nos queremos registrar, y (cuestión realmente importante), una contraseña “maestra” que nos va a permitir tener que recordarla

Unidad 6.

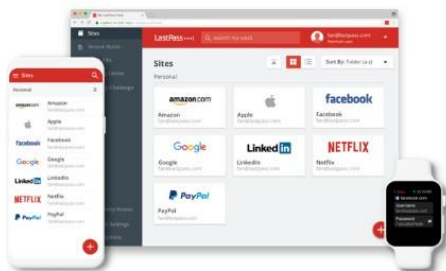
Servicios básicos en la nube: Gestión de Contraseñas en línea

si acaso, solamente a ella, para poder gestionar desde allí las demás que vayamos añadiendo ya con una cuenta en el servicio. Esta contraseña maestra solicita varios requisitos mínimos, como mencionamos antes, que incluyen varios caracteres, números, letras en mayúsculas y minúsculas, con una verificación en tiempo real de la fortaleza de la contraseña:

LastPass

Una contraseña. Sin complicaciones.

| LastPass se encarga del resto.



Funciones de LastPass Free

- ✓ Bóveda de contraseñas segura ⓘ
- ✓ Acceso desde un tipo de dispositivo ⓘ
- ✓ Uso compartido con una persona ⓘ

[o Iniciar sesión](#)

E-mail
 pruebamitic2021@gmail.com

Contraseña maestra

Seguridad

Nuestros requisitos mínimos:

- ✓ 12 caracteres como mínimo
- ✓ Al menos un número
- ✓ Al menos una letra en minúscula
- ✓ Al menos una letra en mayúscula
- ✓ No puede ser su e-mail

Nuestro consejo:

Cuente una historia que resulte única para usted. *Pipolsecomiomisdeberes2*

[¿Cómo debe ser una contraseña para que sea segura?](#)

Confirme la Contraseña Maestra

Una vez seguimos las instrucciones dadas, damos clic al botón de registrar, y se crea la cuenta para que podamos utilizar el servicio. Luego, seguimos las instrucciones dependiendo del navegador que estuviésemos utilizando; en el caso de utilizar Google Chrome, debemos instalar una “extensión” siguiendo las instrucciones en pantalla; básicamente, inicialmente darle clic al botón “Instalar LastPass” y luego de ello, al botón “Añadir a Chrome”.

LastPass

✓ Su cuenta se ha creado correctamente.

ENHORABUENA

Le damos la bienvenida a LastPass.

Instale la extensión para el navegador e inicie sesión con la cuenta que acaba de crear.

Instalar LastPass

Añadir al navegador

Iniciar sesión

Inicio > Extensiones > LastPass: Free Password Manager

Destacados

★★★★★ 29.851 | Productividad | 10.000.000+ usuarios

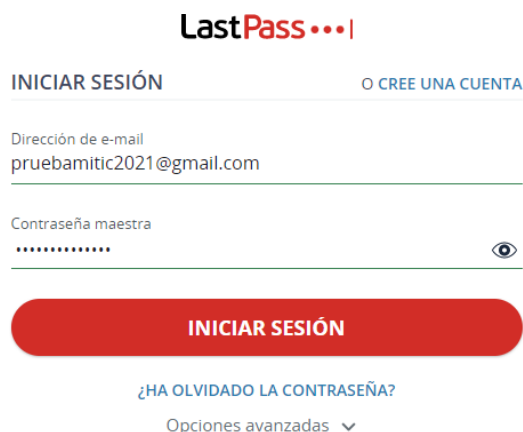
LastPass: Free Password Manager

Añadir a Chrome

Unidad 6.

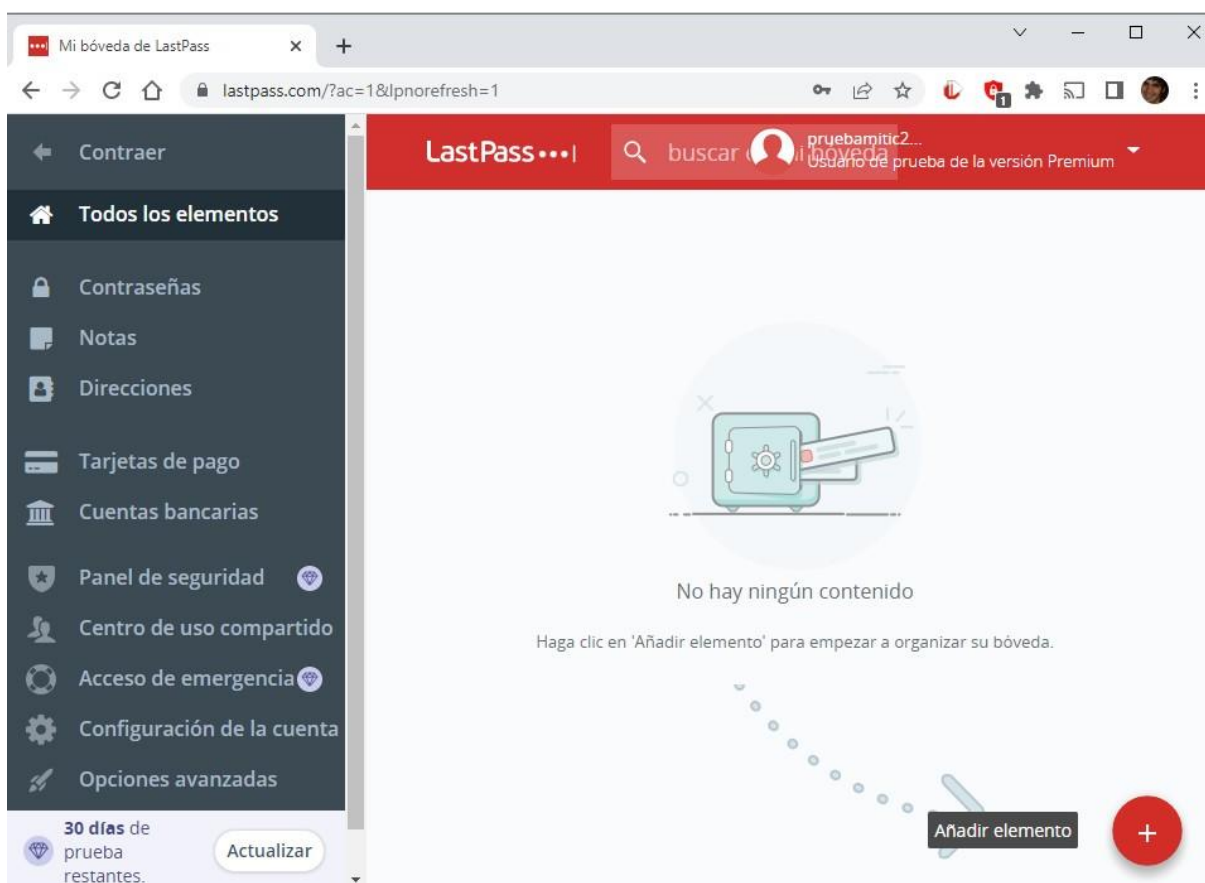
Servicios básicos en la nube: Gestión de Contraseñas en línea

Nada más ya nos queda iniciar sesión desde la página principal del servicio, con las credenciales que hemos creado antes:



The image shows the LastPass login page. At the top is the LastPass logo. Below it are two links: "INICIAR SESIÓN" and "O CREE UNA CUENTA". There are two input fields: "Dirección de e-mail" with the value "pruebamitic2021@gmail.com" and "Contraseña maestra" with masked dots. A red "INICIAR SESIÓN" button is below the fields. Underneath the button are links for "¿HA OLVIDADO LA CONTRASEÑA?" and "Opciones avanzadas".

En la pantalla principal del servicio, se pueden configurar todas las contraseñas necesarias, además de otros elementos adicionales como Notas, Tarjetas o medios de pago, y hasta cuentas bancarias.



Dando clic al botón “Añadir Elemento” y luego configurando uno de ellos, por ejemplo una nueva contraseña, vamos almacenando los elementos que fuésemos necesitando:

Unidad 6.

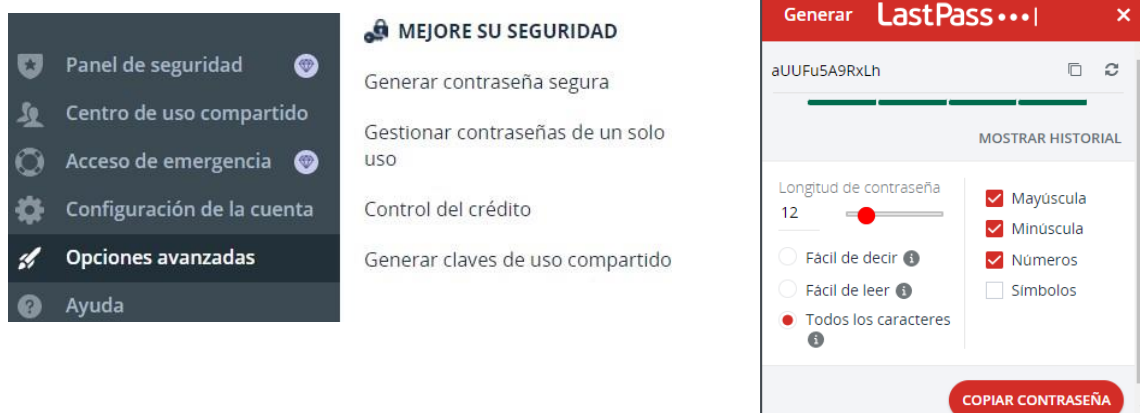
Servicios básicos en la nube: Gestión de Contraseñas en línea



En este ejemplo, creamos una contraseña manual, pero si quisiéramos generar una contraseña aleatoria, no hay más que utilizar el generador de contraseñas aleatorias, ubicado en la herramienta “Opciones Avanzadas” en el menú lateral izquierdo inferior, y luego seleccionando la opción “Generar contraseña segura”. Una vez la seleccionamos, se nos abre una ventana contextual en donde se genera una clave totalmente aleatoria, segura, y que podremos copiar para guardar en alguna credencial de acceso que creásemos, por ejemplo, reemplazando la colocada con el paso anterior, con el botón de copiado y pegando en el cuadro correspondiente.

Unidad 6.

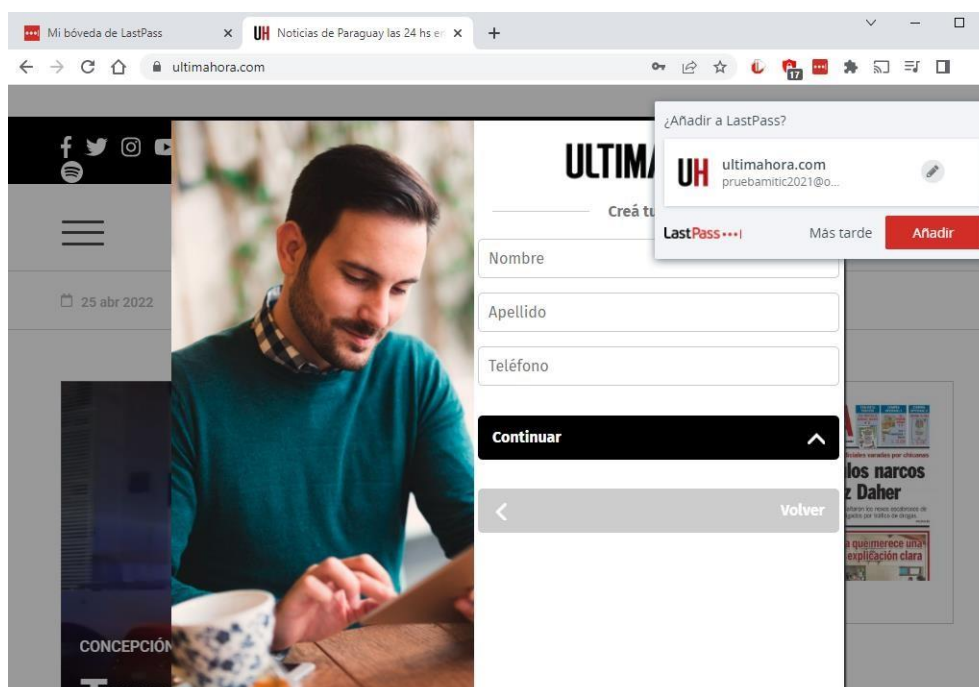
Servicios básicos en la nube: Gestión de Contraseñas en línea



La contraseña segura puede ser configurada para que sea fácil de decir, o bien de leer, o bien que contenga todos los caracteres seleccionados: mayúscula, minúscula, números o bien símbolos, según sea nuestra preferencia para algún sitio en cuestión.

Debemos terminar de alistar la configuración de algún sitio, con o sin contraseña generada (es decir, puede ser una contraseña segura que ya hayamos tenido previamente en el sitio, o bien cambiarla por la que nos generó LastPass a través del procedimiento del sitio en cuestión) dándole clic al botón de guardado, luego de asegurarnos que todo esté correcto.

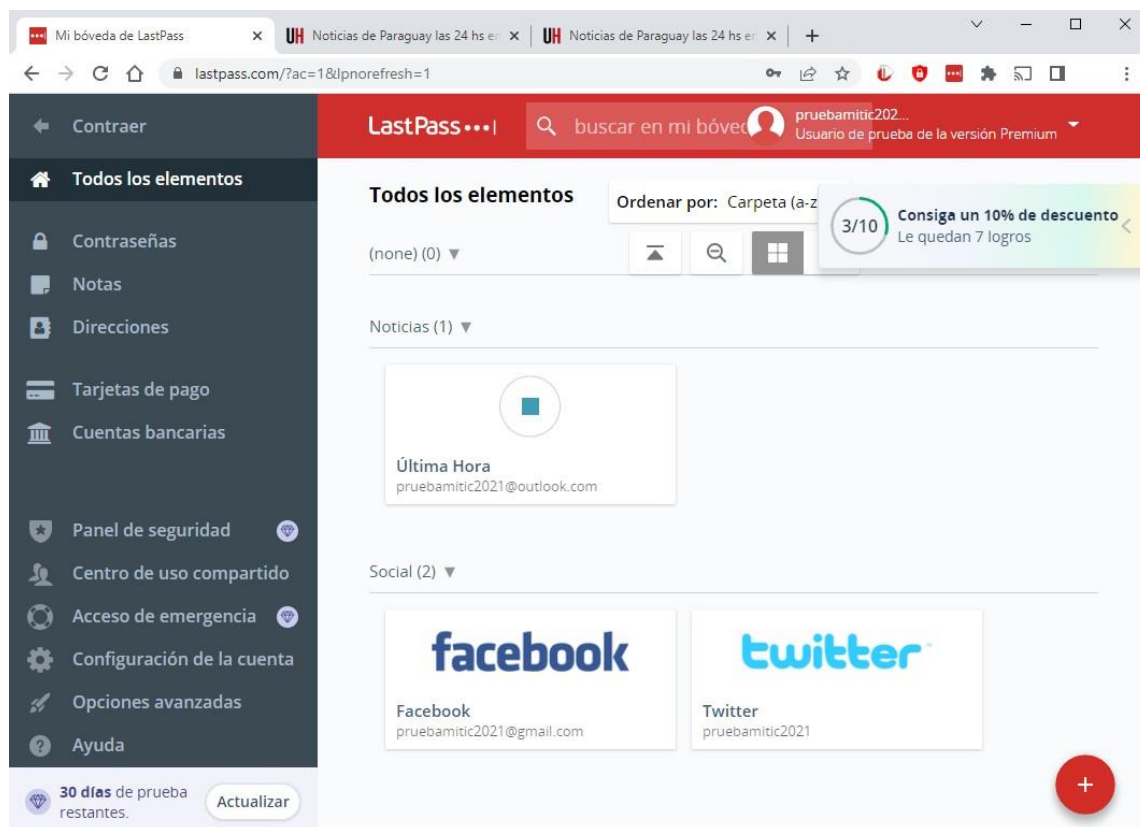
Una vez iniciada la sesión en algún sitio por los procedimientos normales, generalmente la extensión de LastPass (el ícono de tres puntos con fondo rojo) nos pregunta si deseamos añadirla al servicio, o bien en la barra de navegación al hacer clic en dicho ícono nos permite añadir fácilmente el sitio, o bien podemos hacerlo directamente desde el gestor de LastPass antes visto.



Unidad 6.

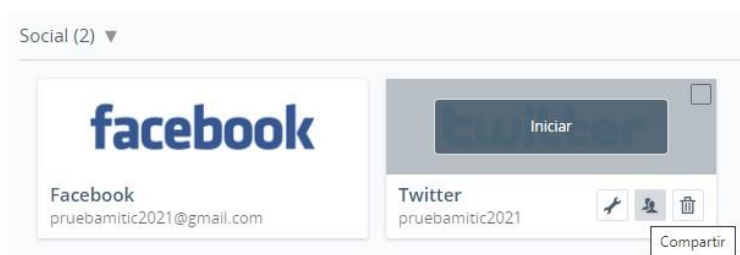
Servicios básicos en la nube: Gestión de Contraseñas en línea

Desde el menú principal del servicio podremos gestionar las contraseñas que tengamos almacenadas, y en caso de querer utilizar alguna, directamente hacemos clic sobre el botón en cuestión y se nos redirige al sitio:



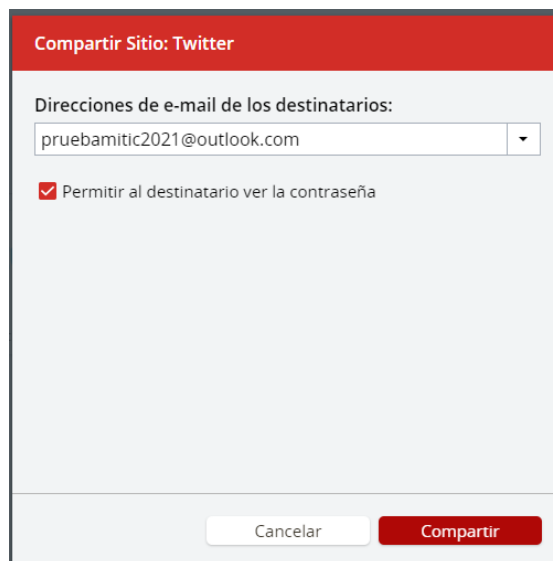
Respecto a la “advertencia” de los días de prueba restante, o de ser usuario de prueba de la versión Premium, es sólo el modelo de negocios de LastPass; realmente, cuando llegan los 30 días, se pasa realmente a la versión Free, con algunas menos capacidades, pero todo lo básico arriba mencionado permitido.

Una cuestión importante es que también podemos compartir las contraseñas que tengamos, de forma segura, con otra persona; para ello dicha persona también debe tener cuenta en LastPass, y en un elemento dado, se debe hacer clic en la herramienta “Compartir” (el botón de amigos que aparece al poner el cursor encima del elemento), luego se debe colocar la dirección de correo de la persona en cuestión, y permitirle ver la contraseña, o simplemente compartirla sin que pueda verla.



Unidad 6.

Servicios básicos en la nube: Gestión de Contraseñas en línea



Compartir Sitio: Twitter

Direcciones de e-mail de los destinatarios:

pruebamitic2021@outlook.com

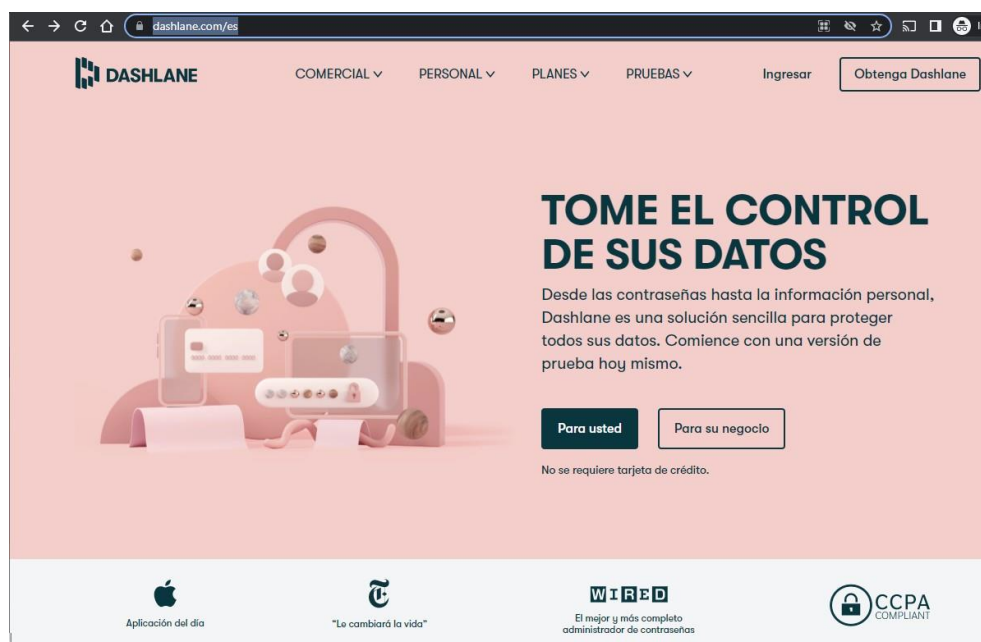
☒ Permitir al destinatario ver la contraseña

Cancelar Compartir

El elemento en cuestión aparecerá también ahora en la cuenta de LastPass del destinatario, y la contraseña habrá sido compartida de forma segura (NO es un medio seguro enviarse contraseñas por mensajes de texto, correo electrónico, aplicaciones móviles, o bien incluso mensajería de redes sociales; no está recomendado hacerlo, y sí se aconseja hacerlo por este tipo de métodos).

Los métodos específicos pueden variar, y también las posibilidades, pero básicamente cualquier gestor de contraseñas gratuito (o en su versión paga, con mayores recursos) puede realizar las acciones que comentamos arriba para el caso específico del servicio de LastPass.

El segundo servicio interesante de este tipo, y que lo vamos a analizar, es el de “**Dashlane**” (<https://www.dashlane.com/es>), que es una solución de gestión de contraseñas en línea que también tiene sus versiones tanto la gratuita como así la de pago.



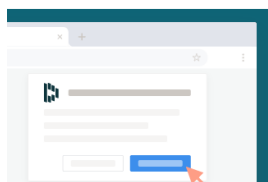
Unidad 6.

Servicios básicos en la nube: Gestión de Contraseñas en línea

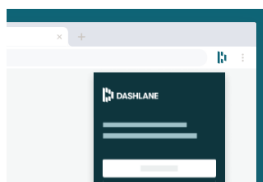
Desde la página inicial, debemos darle al botón “Obtenga Dashlane”, luego instalar la extensión para el navegador que utilicemos (en nuestro caso, el Chrome), luego instalar la extensión con proceso similar al hecho con el anterior servicio (se le da clic en “Agregar a Chrome” y se siguen los pasos indicados).

PRÓXIMA PARADA: CHROME WEB STORE

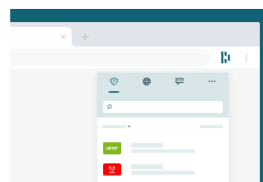
Paso 1: Agregue la extensión



Paso 2: Cree su cuenta



Paso 3: ¡Use Dashlane!



¿No ha sido redirigido? [Haga clic aquí.](#)

[Página principal](#) > [Extensiones](#) > Dashlane - Password Manager



Dashlane - Password Manager

[dashlane.com](#) [Destacado](#)

★★★★★ 2,063 | Productividad | 5,000,000+ usuarios

Agregar a Chrome

Luego de instalar la extensión, somos redirigidos a una página de creación de cuenta, y deberemos ingresar el correo electrónico deseado para asociarlo a la gestión de las contraseñas, y dar clic en “Siguiente”.

LE DAMOS LA BIENVENIDA A DASHLANE EN LA WEB

Acceda a sus contraseñas y datos personales en la aplicación web de manera rápida y segura.

Empiece a usar Dashlane gratis

Escriba el correo electrónico que desea asociar con su cuenta de Dashlane.

Correo electrónico

pruebamitic2021@gmail.com

Siguiente

Debemos crear también una contraseña maestra, recordando que debe cumplir ciertos criterios que antes bien analizamos: incluir en lo posible números, letras alternando mayúsculas y minúsculas, y también símbolos; esta contraseña es la que nos permite utilizar el servicio así que deberemos recordarla con precisión como bien se advierte, si bien será la única necesaria pues del resto se encargará el servicio.

Unidad 6.

Servicios básicos en la nube: Gestión de Contraseñas en línea

Cree una contraseña maestra segura y fácil de recordar

No guardamos su contraseña maestra, así que usted debe recordarla.

CONTRASEÑA

¡Vaya! Ahora sí es segura.

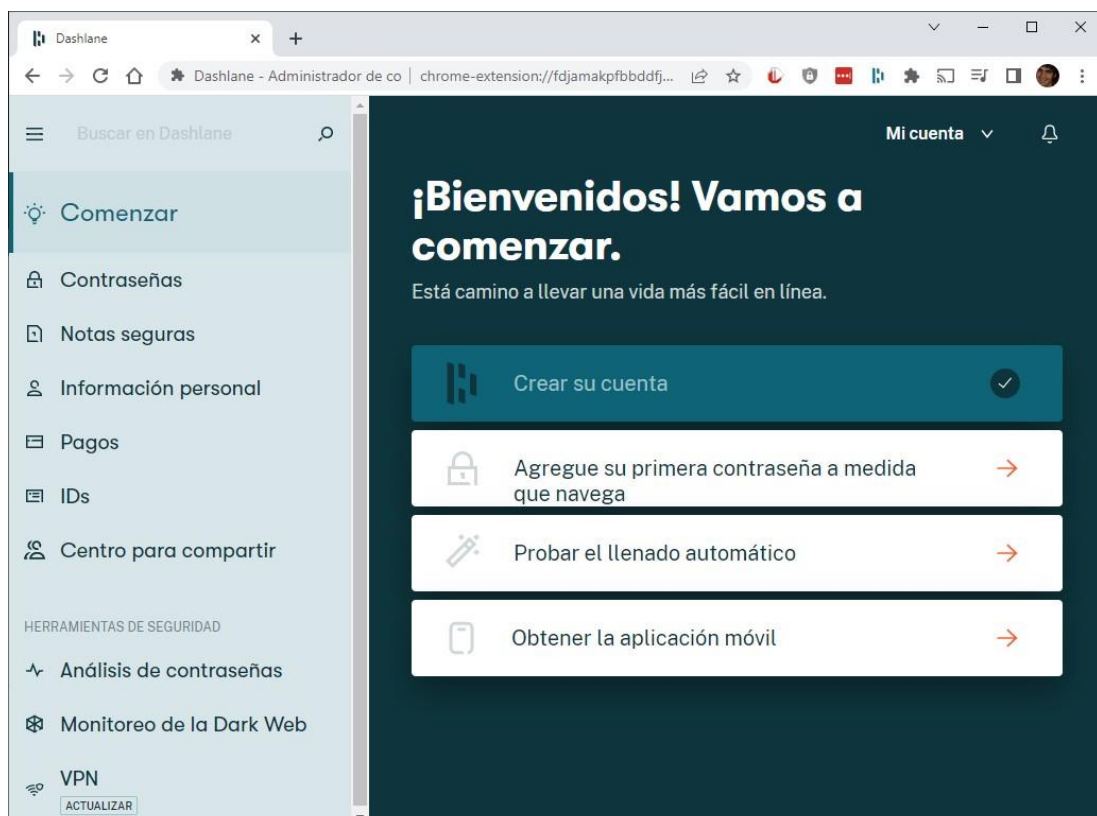
INTRODUZCA NUEVAMENTE SU CONTRASEÑA MAESTRA

☒ Quiero recibir correos electrónicos con sugerencias útiles y ofertas especiales de Dashlane.

[← Atrás](#)

[Crear Mi Cuenta](#)

Tendremos la opción de agregar contraseñas, llenar automáticamente credenciales de inicio, y demás; en la versión básica vamos a centrarnos en la gestión de passwords seguros. Incluso, la primera vez que ingresamos, tenemos un menú interactivo donde nos ofrece crear la primera contraseña, y probar algunas características. En todo caso, siempre podremos agregar contraseñas desde el menú contextual de la izquierda (“Contraseñas”), y luego agregar o gestionar las que tengamos.



Unidad 6.

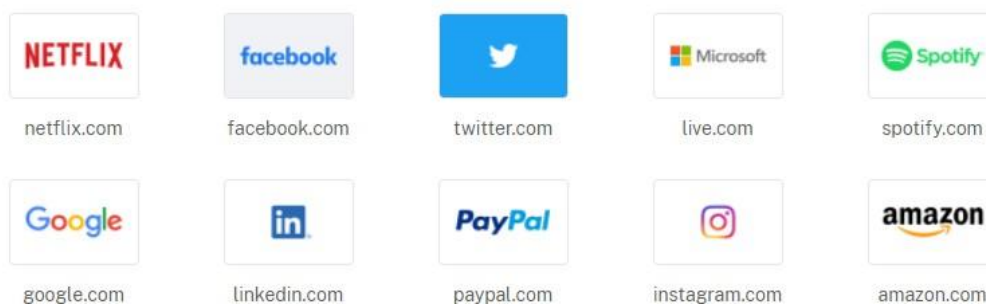
Servicios básicos en la nube: Gestión de Contraseñas en línea

La primera vez tenemos una selección de servicios web populares: Netflix, Facebook, Amazon, Twitter, Spotify e Instagram, entre otros.

←  Agregue su primera contraseña

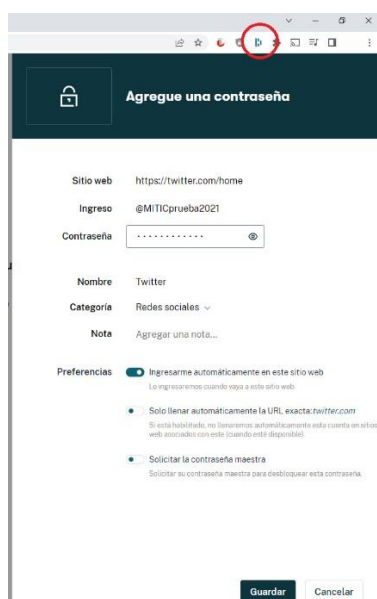
Seleccione un sitio web que use, luego lo ayudaremos a guardarlo.

Será muy fácil, se lo prometemos.



En el ejemplo, seleccionaremos a Twitter, ingresando las credenciales necesarias. Incluso se ofrece una guía de acción, como entrar al sitio web, cerrar momentáneamente sesión, para luego introducir las credenciales de nuevo y guardarlas en Dashlane cuando se ofrezca la posibilidad de hacerlo.

También podemos agregar las contraseñas manualmente desde la extensión de Dashlane en la barra de navegación (una letra “D” pintada en verde oscuro), y rellenando allí los cambios.



Unidad 6.

Servicios básicos en la nube: Gestión de Contraseñas en línea

Finalmente, también podremos gestionar las contraseñas guardadas, editarlas desde la página de contraseñas del servicio, o bien incluso compartirlas desde el menú contextual (tres puntos horizontales en la zona derecha), así como se podía en el anterior servicio.



Para poder compartir las contraseñas de forma segura, se requiere que el destinatario también posea una cuenta en Dashlane, e introducir su dirección de correo electrónico y seguir las instrucciones, pudiendo incluso dar permisos de edición y compartición a los destinatarios.

¿Con quién quiere compartir estos artículos?

Introduzca un correo electrónico o el nombre de un grupo

☒

pruebamitic2021@outlook.com

☐ Mostrar solamente personas seleccionadas

Agregar más artículos

Siguiente

Seleccione el tipo de permiso

☐ **Derechos limitados**

Las personas con derechos limitados solo pueden usar los elementos compartidos con Dashlane. No pueden editar o compartir los elementos compartidos ni revocar el acceso a estos.

☒ **Plenos derechos**

Las personas con plenos derechos tienen la propiedad conjunta de los elementos compartidos. Pueden utilizar, ver, editar y compartir dichos elementos, y revocar el acceso a estos. También pueden revocar su acceso.

Atrás

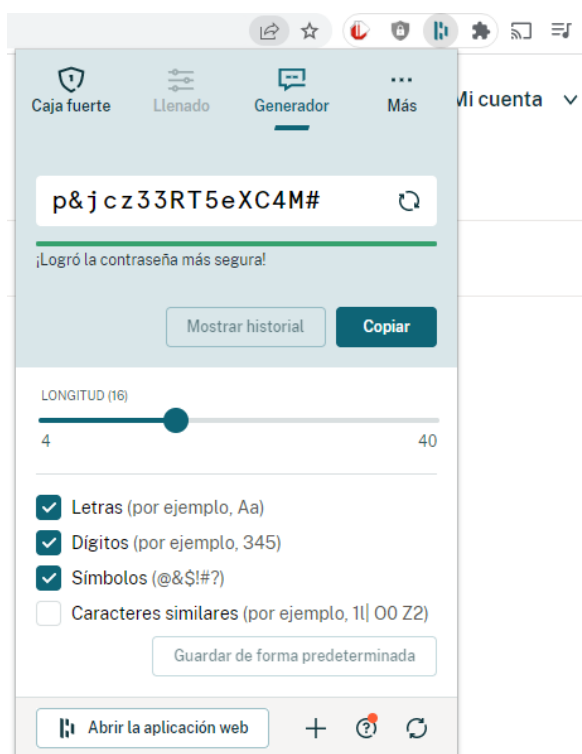
Compartir

Unidad 6.

Servicios básicos en la nube: Gestión de Contraseñas en línea

Se recibe una confirmación de que el archivo se compartió correctamente (en caso de que no haya problemas) y con ello se completa la operación, quedando a disposición del destinatario.

Importante destacar que desde la extensión de Dashlane (la letra D en verde que habíamos mencionado) también se pueden generar nuevas contraseñas seguras, con los parámetros que decidamos, y copiarlas y almacenarlas para el servicio que nos sea conveniente, así como lo hemos visto con el otro servicio antes analizado.



Con todas estas consideraciones, cerramos el análisis básico de este tipo de servicios, con un panorama general de las posibilidades y recursos a disposición, que mejoran enormemente la seguridad y el manejo y gestión de nuestras contraseñas, si son correctamente utilizados.

Unidad 6.**Servicios básicos en la nube: Gestión de Contraseñas en línea****4. Referencias**

Síntesis de material propio por parte de los Docentes.